What is claimed is:

1. A method for preventing cloning of an electronic device, said method comprising steps of:

generating a first electronic signature from a first identification code and a second identification code, the second identification code being suitable for uniquely identifying a hardware component of the electronic device;

decrypting an encrypted electronic signature for generating a second electronic signature;

comparing the first electronic signature and the second electronic signature; and

departing from normal operation of the electronic device if the first electronic signature and the second electronic signature differ.

2. The method as claimed in claim 1, further comprising retrieving the encrypted electronic signature, the first identification code and the second identification code from a non-volatile memory.

3. The method as claimed in claim 1, wherein generating the first electronic signature comprises using a hash function for computing the first electronic signature from the first identification code and the second identification code.

4. The method as claimed in claim 3, wherein the hash function comprises an MD5 algorithm.

5. The method as claimed in claim 1, wherein decrypting the encrypted electronic signature further comprises using a decryption key.

6. The method as claimed in claim 4, wherein the encrypted electronic signature is encrypted using a public key encryption algorithm and the decryption key comprises a public key.

7. The method as claimed in claim 6, wherein the public key encryption algorithm comprises a "$c = m^e \bmod n$" public key encryption algorithm.

8. The method as claimed in claim 1, wherein the first identification code comprises an electronic serial number (ESN).

9. The method as claimed in claim 1, wherein the hardware component comprises a non-volatile memory of the electronic device and the second identification code comprises an identification code suitable for uniquely identifying the non-volatile memory.

10. The method as claimed in claim 1, wherein the hardware component comprises a non-volatile flash memory, and the second identification code comprises a flash hardware serial number permanently stored in the flash memory.

11. The method as claimed in claim 1, wherein the hardware component comprises a processor of the electronic device and the second identification code comprises an identification code suitable for uniquely identifying the processor.

12. The method as claimed in claim 1, wherein departing from normal operation of the electronic device comprises inhibiting normal use of the electronic device.

13. The method as claimed in claim 1, wherein departing from normal operation of the electronic device comprises allowing normal use of the electronic device while providing a warning to at least one of a user of the electronic device and a network in which the device is used that the electronic device has been used to clone a second electronic device.

14. A method for preventing a first non-volatile memory of a first electronic device from being cloned to a second non-volatile memory of a second electronic device, the method comprising steps of:

retrieving a first identification code from the first electronic device, the first identification code for uniquely identifying a hardware component of the first electronic device;

assigning a second identification code for the first electronic device, the second identification code for uniquely identifying the first electronic device;

generating an electronic signature from the first identification code and the second identification code;

encrypting the electronic signature; and

storing the encrypted electronic signature and the second identification code to the first non-volatile memory, the encrypted electronic signature and the second identification code being used for departing from normal operation of the second electronic device if the second non-volatile memory is cloned from the first non-volatile memory.

15. The method as claimed in claim 14, wherein generating the electronic signature comprises using a hash function for computing the electronic signature from the first identification code and the second identification code.

16. The method as claimed in claim 15, wherein the hash function comprises an MD5 algorithm.

17. The method as claimed in claim 14, further comprising storing a decryption key to the first non-volatile memory for decrypting the encrypted electronic signature.

18. The method as claimed in claim 17, wherein the encrypted electronic

signature is encrypted using a public key encryption algorithm and the decryption key comprises a public key.

19. The method as claimed in claim 18, wherein the public key encryption algorithm comprises a "$c = m^e \bmod n$" public key encryption algorithm.

20. The method as claimed in claim 14, further comprising:

retrieving a third identification code from the second non-volatile memory, the third identification code for uniquely identifying the second non-volatile memory;

generating a second electronic signature from the second identification code and the third identification code;

retrieving the encrypted electronic signature from the second non-volatile memory;

decrypting the encrypted electronic signature for generating a third electronic signature;

comparing the second electronic signature and the third electronic signature; and

thereafter departing from normal operation of the second electronic device if the second electronic signature and the third electronic signature differ.

21. The method as claimed in claim 20, wherein generating the second electronic signature comprises using a hash function for computing the second electronic signature from the second identification code and the third identification code.

22. The method as claimed in claim 21, wherein the hash function comprises an MD5 algorithm.

23. The method as claimed in claim 14, wherein the first and second non-volatile memories comprise flash memories, and the first and third identification codes comprise flash hardware serial numbers permanently stored in the flash memories.

24. The method as claimed in claim 23, wherein the second identification code comprises an electronic serial number (ESN).\

25. An electronic device, comprising:

a non-volatile memory; and

a controller for controlling operation of the electronic device,

wherein the controller is suitable for generating a first electronic signature from a first identification code and a second identification code, the first identification code being suitable for uniquely identifying a hardware component of the electronic device; decrypting an encrypted electronic signature for generating a second electronic signature; comparing the first electronic signature and the second electronic signature, and causing the electronic device to depart from normal operation if the first electronic signature and the second electronic signature differ.

26. The electronic device as claimed in claim 25, wherein the controller retrieves the encrypted electronic signature, the first identification code and the second identification code from at least one of the non-volatile memory and a second non-volatile memory of the electronic device.

27. The electronic device as claimed in claim 25, wherein the controller generates the first electronic signature using a hash function.

28. The electronic device as claimed in claim 27, wherein the hash function comprises an MD5 algorithm.

29. The electronic device as claimed in claim 25, wherein the controller employs a decryption key for decrypting the encrypted electronic signature.

30. The electronic device as claimed in claim 25, wherein the encrypted electronic signature is encrypted using a public key encryption algorithm and the decryption key comprises a public key.

31. The electronic device as claimed in claim 30, wherein the public key encryption algorithm comprises a "$c = m^e \bmod n$" public key encryption algorithm.

32. The electronic device as claimed in claim 25, wherein the non-volatile memory comprises a flash memory, and the first identification code comprises a flash hardware serial number permanently stored in the flash memory.

33. The electronic device as claimed in claim 25, wherein the second identification code comprises an electronic serial number (ESN).

34. An electronic device, comprising:

means for generating a first electronic signature from a first identification code and a second identification code, the first identification code being suitable for uniquely identifying a hardware component of the electronic device;

means for decrypting an encrypted electronic signature for generating a second electronic signature;

means for comparing the first electronic signature and the second electronic signature, and

means for departing from normal operation of the electronic device if the first electronic signature and the second electronic signature differ.

35. The electronic device as claimed in claim 34, wherein the non-volatile memory comprises a flash memory, and the first identification code comprises a flash hardware serial number permanently stored in the flash memory.

36. The electronic device as claimed in claim 34, wherein the second

identification code comprises an electronic serial number (ESN).